



VIEW Certified Configuration Guide

Nortel

WLAN Security Switch 2300 Series with AP-2330

June 2008 Edition 1725-36082-001 Version G

Trademark Information

Polycom® and the logo designs SpectraLink® LinkPlus Link NetLink SVP

Are trademarks and registered trademarks of Polycom, Inc. in the United States of America and various countries. All other trademarks used herein are the property of their respective owners.

Patent Information

The accompanying product is protected by one or more US and foreign patents and/or pending patent applications held by Polycom, Inc.

Copyright Notice

Copyright © 2005 to 2008 Polycom, Inc.

All rights reserved under the International and pan-American copyright Conventions.

No part of this manual, or the software described herein, may be reproduced or transmitted in any form or by any means, or translated into another language or format, in whole or in part, without the express written permission of Polycom, Inc.

Do not remove (or allow any third party to remove) any product identification, copyright or other notices.

Every effort has been made to ensure that the information in this document is accurate. Polycom, Inc. is not responsible for printing or clerical errors. Information in this document is subject to change without notice and does not represent a commitment on the part of Polycom, Inc.

Notice

Polycom, Inc. has prepared this document for use by Polycom personnel and customers. The drawings and specifications contained herein are the property of Polycom and shall be neither reproduced in whole or in part without the prior written approval of Polycom, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Polycom reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Polycom to determine whether any such changes have been made.

No representation or other affirmation of fact contained in this document including but not limited to statements regarding capacity, response-time performance, suitability for use, or performance of products described herein shall be deemed to be a warranty by Polycom for any purpose, or give rise to any liability of Polycom whatsoever.

Contact Information

Please contact your Polycom Authorized Reseller for assistance.

Polycom, Inc. 4750 Willow Road, Pleasanton, CA 94588 http://www.polycom.com

Introduction

Polycom's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between SpectraLink Wireless Telephones and wireless LAN (WLAN) infrastructure products.

The products listed below have been thoroughly tested in Polycom's lab and have passed VIEW Certification. This document details how to configure the Nortel WLAN Security Switch 2300 Series and WLAN AP-2330/2330A/2330B with SpectraLink Wireless Telephones.

Manufacturer:	Nortel: www.nortel.com				
Approved products:	WLAN Security Switc	hes	Access points		
	2380		2330 [†]		
	2361 [†]		2330A		
	2360		2330B		
	2350				
Security:	WPA-PSK and WPA2-PSK				
2300 software version certified:	Release 5.0.11.4				
SpectraLink handset models certified: **	e340/h340/i640	8020/8030		8030	
SpectraLink handset software certified:	89.119	122.010 or greater			
SpectraLink radio mode:	802.11b	802.11b 802.11a		802.11a	
Maximum telephone calls per AP:	10 10 12		12 *		
Recommended network topology:	Switched Ethernet (required)				

Certified Product Summary

[†] Denotes products directly used in Certification testing.

* Maximum calls tested during VIEW Certification. The certified product may actually support a higher number of maximum calls for 802.11a radio modes.

** SpectraLink handset models 8020/8030, e340/h340/i640 and their OEM derivates are VIEW Certified with the WLAN hardware and software identified in the table. Throughout the remainder of this document they will be referred to collectively as "SpectraLink Wireless Telephones".

Service Information



The access point (AP) must support SpectraLink Voice Priority (SVP). Contact your AP vendor if you need to upgrade the AP software.

Contacting Nortel Technical Support

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Additional information about the Nortel Technical Solutions Centers is available from <u>http://www.nortel.com/contactus</u>.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to http://www.nortel.com/erc.

If you purchased a Nortel service program, contact one of the following Nortel Technical Solutions Centers:

Europe, Middle East, and Africa - 00800 8008 9009 or +44 (0) 870 907 9009 North America - (800) 4NORTEL or (800) 466-7835

Asia Pacific - (61) (2) 9927-8800

China - (800) 810-5000

Known Limitations

During VIEW Certification testing, the following limitations were discovered.

- RF Active Scan must be disabled on AP radios that are providing voice services, including SpectraLink Wireless Telephones.
- You must disable Internet Group Management Protocol (IGMP) snooping when running SpectraLink Radio Protocol (SRP), which is used with the SpectraLink 8000 Telephony Gateway. SRP uses multicast packets to do an SRP Check-In, which are not forwarded through the WLAN Security Switch (WSS) when IGMP snooping is enabled. When a tunneled virtual LAN (VLAN) is configured over a Layer-3 network, IGMP snooping must be disabled each time the tunnel is established, because the virtual VLAN is established with IGMP snooping turned on by default.

Network Topology

The following topology was tested during VIEW Certification. It is important to note that these do not necessarily represent all "Certified" configurations.

Both Layer-2 and Layer-3 roaming were tested. Layer-3 roaming of SpectraLink Wireless Telephones requires the use of a generic routing encapsulation (GRE) tunnel.



Access Point Capacity and Positioning

Please refer to the Polycom <u>Deploying Enterprise-Grade Wi-Fi Telephony</u> white paper. This document covers the security, coverage, capacity and QoS considerations necessary for ensuring excellent voice quality with enterprise Wi-Fi networks.

For more detailed information on wireless LAN layout, network infrastructure, QoS, security and subnets, please see the <u>Best Practices</u> <u>Guide for Deploying SpectraLink 8020/8030 Wireless Telephones</u>. This document identifies issues and solutions based on Polycom's extensive experience in enterprise-class Wi-Fi telephony, and provides recommendations for ensuring that a network environment is adequately optimized for use with SpectraLink 8020/8030 Wireless Telephones.

For setting up the data rates, please consult your facility's RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. SpectraLink Wireless Telephones require the following minimum dBm reading to support the corresponding "Required" data rate setting in the access point.

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Required" Data Rate
902 11b	-70 dBm	1 Mb/s
002.110	-60 dBm	11 Mb/s
902 11a	-63 dBm	6 Mb/s
602.TTY	-47 dBm	54 Mb/s
802 112	-60 dBm	6 Mb/s
002.118	-45 dBm	54 Mb/s



All SpectraLink Wireless Telephones on the WLAN network must be configured for a single radio standard (802.11a, or 802.11b, or 802.11g). Handsets configured for different radio standards will not work together.

Configuring a New WLAN Security Switch Starting from Factory Defaults

- **1.** Using the supplied DB-9 male to DB-9 female standard RS-232 cable, connect the WLAN Security Switch to the serial port of a terminal or PC.
- **2.** Run a terminal emulation program (such as HyperTerminal) or use a VT-100 terminal with the following configuration:

Bits per second:	9600
Data bits:	8
Parity:	None
Stop bits:	1
Flow control:	None

- **3.** Power-on the WLAN Security Switch. The status of the boot process will appear in the console as the switch is powering up. Once the switch is operational you will be presented with a login prompt.
- 4. A Quick Start Wizard provides for an easy means to perform initial WLAN Security Switch setup and configuration. Refer to the WLAN Security Switch 2300 Series Quick Start Guide found at Nortel's Technical Support site. This document contains a detailed explanation of using the Startup Wizard: <u>http://support.nortel.com/go/main.jsp?cscat=DOCDETAIL&id= 583095&poid=16021</u>
- 5. Once the WLAN Security Switch has been configured via the Quick Start Wizard, the remaining configuration can be performed using command line interface (CLI), Web View or WLAN Management Software (WMS). Configuration examples will be provided for both CLI and WMS.
- 6. If necessary, the WLAN Security Switch may be reset to factory defaults. To reset the WLAN Security Switch to factory defaults, you must issue the "clear boot config" command via the console.



Connecting APs

To configure the WLAN Security Switch (WSS) to support an AP, you must first determine how the AP will connect to the switch. There are two types of AP-to-WSS connection: direct and distributed.

Directly connected APs

In direct connection, an AP connects to one or two 10/100 ports on a WSS. The WSS port is then configured specifically for a direct attachment to an AP. There is no intermediate networking equipment between the WSS and AP, and only one AP is connected to the WSS port. The WSS 10/100 port provides power over Ethernet (PoE) to the AP. The WSS also forwards data only to and from the configured AP on that port. The port numbers on the WSS which are configured for directly attached APs reference a particular AP.

Distributed APs

An AP that is not directly connected to a WSS is considered a distributed AP. There may be intermediate Layer 2 switches or Layer 3 IP routers between the WSS and the AP. The WSS may communicate to the distributed AP through any network port. (A network port is any port connecting the switch to other networking devices, such as switches and routers, and it can also be configured for 802.1Q VLAN tagging.) The WSS contains a configuration for a distributed AP based on the AP's serial number. Similar to ports configured for directly connected APs, distributed AP configurations are numbered and can reference a particular AP. These numbered configurations do not, however, reference any physical port.

During VIEW Certification, the 2330 access points were tested while directly connected to a port on the WLAN Security Switch (e.g. port 1), but both methods are supported.



For more information on how to configure the network to support a distributed AP, see the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.

Command, comment, and screen text key

In the sections below you will find commands, comments and system responses or other screen-displayed information involved in the configuration process. This key explains the text styles and symbols used to denote them.

Text Style	Denotes:
xxxxxxx	Typed command
<xxxxxxxx< th=""><th>Encryption key, domain name or other information specific to your system that needs to be entered</th></xxxxxxxx<>	Encryption key, domain name or other information specific to your system that needs to be entered
# xxxxxxxx	Comment about a command or set of commands
xxxxxxx	System response or other displayed information

Configuration Example – CLI

AP configuration

To add a directly connected AP-2330 attached to port 1 on a WSS using CLI:

set port type ap 1 model 2330 poe enable

Defines the port number on the switch that the AP is connected to, the model number of the AP and enables PoE on the switch port. Valid model numbers include the 2330, 2330A and 2330B.

set ap 1 radio 1 tx-power 10 mode enable

Sets the channel number, transmit power and enables the 802.11g radio.

set ap 1 radio 2 channel 44 tx-power 10 mode enable

Sets the channel number, transmit power and enables the 802.11a radio.

To add a distributed AP-2330 to a WSS using CLI:

set dap 1 serial-id stpw20kc3 model 2330

Defines the DAP number, serial-id and model number of the AP. Valid model numbers include the 2330, 2330A and 2330B.

- set dap 1 radio 1 channel 11 tx-power 10 mode enable
 # Sets the channel number, transmit power and enables
 the 802.11g radio.
- set dap 1 radio 2 channel 40 tx-power 10 mode enable
 # Sets the channel number, transmit power and enables
 the 802.11a radio.

VLAN configuration

For security and flexibility it is recommended that voice and data be configured on separate VLANs. For this example a new VLAN named Voice with a VLAN ID 2 will be created and tagged to the uplink port 8:

set vlan 2 name Voice

Creates a new VLAN ID and defines the name.

set vlan 2 port 8 tag 2

Assigns the VLAN to a port and specifies an 802.1Q tag value.

set igmp disable vlan Voice

Disables IGMP on Voice VLAN.

Service profile / SSID configuration

To create a SSID named Voice using WPA-PSK that will be advertised on 802.11a/b/g radios using CLI:

set service-profile Voice ssid-name Voice

Creates a new service profile and SSID named Voice. Note it's a best practice recommendation to use the same name for both the service profile and SSID

set service-profile Voice auth-fallthru last-resort

Sets the authentication type to open authentication. With WPA-PSK the pre-shared key will be used to authenticate the handset.

set service-profile Voice wpa-ie enable

Enables WPA security.

set service-profile Voice psk-phrase <enter-apassphrase>

Defines the passphrase required to access the SSID.

set service-profile Voice auth-psk enable

Enables pre-shared-key authentication.

set service-profile Voice auth-dot1x disable

Disables 802.1x authentication.

set service-profile Voice attr vlan-name Voice # Specifies the VLAN name to map the voice handsets

traffic to.

To create a SSID named Voice using WPA2-PSK that will be advertised on 802.11a/b/g radios using CLI:

set service-profile Voice ssid-name Voice

Creates a new service profile and SSID named Voice. Note it's a best practice recommendation to use the same name for both the service profile and SSID

set service-profile Voice auth-fallthru last-resort

Sets the authentication type to open authentication. With WPA-PSK the pre-shared key will be used to authenticate the handset.

set service-profile Voice rsn-ie enable

Enables WPA2 security.

set service-profile Voice cipher-tkip disable
 # Disables TKIP encryption.

set service-profile Voice cipher-ccmp enable

Enables AES/CCMP encryption.

set service-profile Voice psk-phrase <enter-apassphrase>

Defines the passphrase required to access the SSID. set service-profile Voice auth-psk enable # Enables pre-shared-key authentication.

set service-profile Voice auth-dot1x disable

- # Disables 802.1x authentication.
- set service-profile Voice attr vlan-name Voice
 # Specifies the VLAN name to map the voice handsets
 traffic to.

Radio Profile configuration

The default Radio Profile needs to be modified to disable certain features to support the handsets. To modify the default Radio Profile using CLI:

set radio-profile default service-profile Voice

Maps the voice service profile and SSID to the radio profile. This determines which 802.11 radios advertise and can support voice handsets.

set radio-profile default dtim-interval 3

Sets the DTIM interval to support push-to-talk.

set radio-profile default auto-tune channel-config
disable

Disables automatic channel assignment for radios assigned to the radio profile. A static channel configuration is recommended to provide a stable and optimum RF environment for the handsets.

set radio-profile default active-scan disable

Disables active-scanning which prevents the radios from going off-channel and disrupting voice services.

set radio-profile default qos-mode svp

Sets the QoS mode to SVP. WMM support is not currently available on the SpectraLink Wireless Telephones.

Access control list

To create an access control list (ACL) that allows and prioritizes IP protocol 119 (SVP) with a Class of Service (CoS) 7 and allows all other IP traffic on the Voice VLAN using CLI:

set security acl ip SpectraLink permit cos 7 119 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255

Creates an ACL that matches protocol 119 (SVP) and marks it with a CoS 7.

set security acl ip SpectraLink permit 0.0.0.0
255.255.255

Creates an ACL that matches all traffic and ports.
commit security acl SpectraLink

Commits and applies the ACL.

set security acl map SpectraLink vlan Voice in

set security acl map SpectraLink vlan Voice out

Applies the ACL to the Voice VLAN for ingress and egress traffic.

To create an ACL that allows and prioritizes IP protocol 119 (SVP) with a Class of Service (CoS) 7 and denies all other IP traffic on the Voice VLAN using CLI:

set security acl ip SpectraLink permit cos 7 119 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255

Creates an ACL that matches protocol 119 (SVP) and marks it with a CoS 7

commit security acl SpectraLink

Commits and applies the ACL.

set security acl map SpectraLink vlan Voice in

set security acl map SpectraLink vlan Voice out

Applies the ACL to the Voice VLAN for ingress and egress traffic.

Saving changes

To save the current changes to a WSS using CLI:

save config

Saves all configuration changes to the running configuration file.

Configuration Example – WLAN Management Software

Adding a WLAN Security Switch to the Network Plan

Before WLAN Management Software can be used to configure a WLAN Security Switch, the WSS must be added to the WMS server. To add a WLAN Security Switch to WLAN Management Software:

- 1. Assuming that WMS is installed and a Network Plan has been created, launch the WMS client and connect to the WMS server. For more information, see the *Nortel WLAN Management Software* 2300 Series User Guide.
- 2. In WMS, click **Configuration** on the tool bar.



3. In the Network Plan Tasks panel, under Other select Upload WSS.

- **4.** In the **IP Address** field, type the IP address for the WLAN Security Switch.
- **5.** In the **Enable Password** field, type the enable password for the WLAN Security Switch.



The enable password must match the enable password that was defined in the Quick Start Wizard. For more information, see the *Nortel WLAN Security Switch 2300 Series Configuration Guide*.

- 6. Click the **Next** button. The uploading progress is shown.
- 7. After the **Successfully uploaded device** message is displayed, click the **Next** button.

AP configuration

To add a directly connected or distributed AP to a WLAN Security Switch using WMS:

- **1.** Connect the AP to the network (distributed AP) or a free PoE port on the switch (directly connected AP).
- 2. In WMS click **Configuration** on the tool bar.
- 3. In the Organizer panel, expand the WSS and select Access Points.
- 4. In the Network Plan Tasks panel, create a new AP by selecting Distributed AP or Directly Connected AP.

🙋 WMS 6.0: Plan (Polycor	n)								
<u>File S</u> ervices <u>T</u> ools H	telp								
🗢 🔿			N	3			9	۱	
Back Forward	Policies	RF Planning	Configuration	Verification	Devices	Monitor	Alarms	Reports	
Organizer	4	Polycom					5, 2 2 12	Network Plan Tasks	4
Polycom								WSS2360 Changes	8
⊕-System		Distributed Access Po	ints					Review	
Wireless	<	Security Mode Optional	-						
Radio Profiles	-	Enable Auto AP							
Access Points		AP Number	Name	Serial#	Model	Туре		Create	۲
RF Detection							100	O Distribute of AD	
								 Distributed AP Directly Connected AP 	
								 Directly connected AP 	
		L			Pr	operties De	lete	Setup	8
		Directly Connected Ac	cess Points ——					AP Redundancy	
		Port#	Name		Model	Туре		🔿 Auto AP	
							1		
								Other	۲
								Convert Auto AP	
					Pn	operties De	lete	Remove Auto AP	

5. For directly connected APs, select an available port on the switch from the **Available Ports** drop-down list. Click the **Next** button.

Create Directly Connected AP
AP Port Selection
Select an available port. Connecting the AP to a port removes the port from all VLANs.
Available Ports P01 -
< Previous Next > Finish Cancel

6. For distributed APs, enter the Name and Serial Number of the AP. Click the Next button.

Create Distributed AP
AP Identifier
Enter a number, unique name, and connection for the AP. Connecting the AP to a port removes the port from all VLANs.
AP Number 1 + Name WAP-2330-1 Serial Number stp1w20kc3
Enter the serial number of the AP Fingerprint Enter the fingerprint. A fingerprint is required if a secure connection is used between the WSS and the AP
nter the 16-byte fingerprint using colons (:) to separate each byte.
< Previous Next > Finish Cancel

7. Specify the model of the Nortel AP you are configuring. Valid models include **2330, 2330A** and **2330B**. Click the **Next** button.

🙋 Create Directly Connected AP	
AP Type Select the AP type	
AP Model Radio Type 2330 2330A 2330A 2330B MP-372-JL MP-372-JL MP-372A MP-422	
	< Previous Next > Finish Cancel

- 8. To configure the 802.11g Radio:
 - a. Select **default** for the **Radio Profile**.
 - **b.** Specify the **Channel Number** and **Transmit Power** the radio should use, as determined by the site survey performed on the facility. Click the **Next** button.

🙋 Create Directly Co	nnected AP	\mathbf{X}
802.11g Radio Configure the 802.110	g radio	
Number Enabled Radio Profile Channel Number Transmit Power [dBm]	1 default V 6 V 18 V	
	< Previous Next > Finish Cancel	

- 9. To configure the 802.11a Radio,
 - a. Select default for the Radio Profile.
 - **b.** Specify the **Channel Number** and **Transmit Power** the radio should use, as determined by the site survey performed on the facility.
- **10.** Click the **Finish** button.

🖉 Create Directly Con	inected AP	×
802.11a Radio		
Configure the 802.11a	radio	
Number Enabled Radio Profile Channel Number Transmit Power [dBm]	2 ✔ default ▼ 36 ▼ 19 ★	
	< Previous Next > Finish Cancel	

11. The AP has now been added to the WLAN Security Switch.

VLAN configuration

For security and flexibility it is recommended that voice and data be on separate VLANs. For this example, a new VLAN named **Voice** with a VLAN ID **2** will be created and tagged to the uplink port **8**.

- **1.** In WMS click **Configuration** on the tool bar.
- 2. In the **Organizer** panel, expand the **WSS** and select **VLANs**.
- 3. In the Network Plan Tasks panel, select Create VLAN.

🙋 WMS 6.0: Plan (Polycom)								
<u>Fi</u> le <u>S</u> ervices <u>T</u> ools Help								
🗢 🔶 🚯			3		%	9	٢	
Back Forward Policies	RF Planning	Configuration	Verification	Devices	Monitor	Alarms	Reports	
Organizer 😔	Polycom					5,5 2 12	Network Plan Tasks	4
E Polycom 白WS52360							W552360 Changes	۲
System	VLANs						Poview	
Ports	VLAN Tag Type 8	J2.1Q					Review Deploy	
Management Services	VLAN Name	VLAN ID IP A	Address 🔽 Int	erface En Tunnel A	ffi VLAN Mem		0.000	
Log	1 Data 1	192	. 168 .1.50		5 🜩 P08		Create	۲
VLANs							Create III AN	
ACLs							Create VLAN	
€Wireless								
±—AAA	Spanning Tree Proper	ties —						
	Enable Uplink Fast]						
	Enable Backbone Fast							
		Config: 0 E	Errors; 3 Warnings	Local Changes: none	e Network Changes: no	ne Alari	ms 1 0 0 0 :	

- 4. For VLAN Name enter Voice.
- 5. For VLAN ID specify 2. Click the Next button.

🙆 Create VLAN
VLAN Identifier
Enter a unique name to identify the VLAN. You can also change the VLAN number.
VLAN Name Voice
Updated [VLAN Name] Value [Voice]
< Previous Next > Finish Cancel

- 6. In the **Port/Port Group** list, select the 802.1Q tagged uplink port (**P08**) and click the **Add** button.
- 7. Click the **Tag** check box and specify the 802.1Q tag value **2**.
- 8. Click the **Finish** button.

Create VLAN	
Optional: VLAN Members	
You can select one or more ports/port-groups to be members of the VLAN.	
Port/Port Group VLAN(s) P02 P03 P03 P04 P05 P05 P06 P06 P07 Move P	Port/Port Group Tag Tag Value
1>	Previous Next > Finish Cancel

- 9. The Voice VLAN 2 is now 802.1Q tagged to the uplink port P08.
 - **a.** Highlight the **Voice** VLAN.
 - b. In the Network Plan Tasks panel, select IGMP.

Elie Services Loois Help Back Forward Policies RF Planning Configuration Verfication Devices Monitor Alarms Reports Organizer Polycom Portorson - Wos22360 Port Groups - Ports Port Groups - Port Groups VLAN Ing Type @02.10 VLAN Ing Type @02.10 VLAN Ing Type @02.10 VLAN Ing Type @02.10 Port Groups VLAN Ing Type @02.10 Port Groups VLAN Ing Type @02.10 Port Groups VLAN Ing Type @02.10 Port Groups VLAN Ing Type @02.10 VLAN I	🙋 WMS 6.0: Plan (Polycor	om)								2
Back Forward Poldes RF Planning Configuration Verification Devices Montor Alarms Reports Organizer Organizer Organizer Polycom Save Decard Network Plan Tasks Image: Save Decard UNAN Source Struces Ports Ports VLAN Tog Type [802.10] Image: Save Decard WS52360 Changes Image: Save Decard ULAN Tog Type [802.10] VLAN Tog Type [802.10] Image: Save Decard WS52360 Changes Image: Save Decard ULAN Tog Type [802.10] VLAN Tog Type [802.10] Image: Save Decard Image: Save Decard Image: Save Decard ULAN Tog Type [802.10] VLAN Tog Type [802.10] Image: Save Decard Image: Save Decard Image: Save Decard ULAN Tog Type [802.10] VLAN Tog Type [802.10] Image: Save Image: Save Decard Image: Save Decard ULAN Tog Type [802.10] Image: Save VLAN Tog Type [802.10] Image: Save Decard Image: Save Decard Image: Data Image: Image: Save Image: Save Image: Save Decard Image: Save Image: Save Image: Save Image: Data Image: Save Image: Data Image: Save Image: Data Image: Save <	<u>File S</u> ervices <u>T</u> ools H	Help								
Back Forward Polices RF Planning Configuration Verification Devices Montor Alarms Reports Organizer Polycom Polycom Save Decord Verification Verification Verification Devices Montor Alarms Reports Polycom Save Decord Verification Save Decord VS52360 Changes VS52360 Changes Polycon Deploy Create Review Deploy Deploy Create Review Deploy Deploy Create Review Deploy Create <t< td=""><td>🦕 📦</td><td></td><td>(The second sec</td><td>1</td><td>X</td><td></td><td>5</td><td>0</td><td><u>ک</u></td><td></td></t<>	🦕 📦		(The second sec	1	X		5	0	<u>ک</u>	
Organizer Połycom Save Network Plan Tasks Połycom Save Discard WS52360 Changes Image: Save WS52360 Changes Image: Save WS52360 Changes Image: Save Discard WS52360 Changes Image: Save Image: Save Discard Image: Save WS52360 Changes Image: Save Image:	Back Forward	Policies	RF Planning	Configuration	Verification	Devices	Monitor	Alarms	Reports	
Polycom B-WS2360 B-System Ports Port Groups Management Services Port Groups Management Services Port Groups Management Services VLAN Name VLAN ID I Data 1 1 Data 1 2 Voice 2 I Data 1 1 Data 1	Organizer	40	Polycom					5.7 2 12	Network Plan Tasks	42
E-WS22360 → System → Ports → Port Groups → Management Services → VLAN Tag Type 802.1Q → Port Groups → Management Services → VLAN Name → VLAN D IP Address Interface E Turnel Affi ↓ UAN Mem Q below → UAN Services → VLAN Name ↓ UAN Setup ↓ Create ↓ Create ↓ Create ↓ UAN Setup ↓ UAN Members ↓ Spanning Tree ↓ UAN Members ↓ Spanning Tree ↓ UAN Members ↓ Spanning Tree ↓ UAN Members ↓ Spanning Tree ↓ IGMP ↓ Restrict L2 Traffic ↓ Restrict L2 Traffic	툴 Polycom								WEE22E0 Chappen	
YLANS YLANS Ports Ports Port Groups YLAN Name YLAN ID IP Address Log Interface E, Turnel Affi YLANS Imagement Services Log Imagement Services YLANS Imagement Services YLANAS Imagement Services Properties Imagement Services Imagement Services	⊡₩552360								w352360 changes	~
VLAN Tag Type 802.1Q Interface E Tunnel Affi VLAN Mem Management Services 1 Log 1 P Services 1 VLAN Services 1 Vertess 2 E-AAA Spanning Tree Properties Enable Uplink Fast Enable Uplink Fast Enable Backbone Fast 0 VLAN Members 3 Spanning Tree Properties 0 Value 0 Value 0 Properties 0 Enable Uplink Fast 0 Enable Backbone Fast 0 Restrict 12 Traffic 0 Restrict 13 Traffic 0	Ports		VLANs						Review	
Management Services ULAN Name VLAN ID IP Address Interface E Tunnel Affi ULAN Mem Image: Construction of the constru	Port Groups		VLAN Tag Type 8	802.1Q					Deploy	
Log 1 12 12 1 1 12 1 1 12 1 1 12 1	Management Ser	ervices	VLAN Name	VLAN ID IP	Address Ir	terface E Tunnel Af	fi VLAN Mem.			
Postvices AcLs QoS Wireless AAA Spanning Tree Properties Enable Uplink Fast Enable Backbone Fast YUAN Mail Properties O Create VLAN Setup O VIAN Members Spanning Tree O Image: Create VLAN Setup O VIAN Members O Image: Create VLAN Setup O VIAN Members O Image: Create VLAN Setup Image: Create VLAN Setup O VIAN Members Image: Create VLAN Image: Create VLAN <td>Log</td> <td></td> <td>1 Data 1</td> <td>19</td> <td>2.168.1.50</td> <td></td> <td>5 - P08</td> <td>16</td> <td>Create</td> <td>(2)</td>	Log		1 Data 1	19	2.168.1.50		5 - P08	16	Create	(2)
ACLS QoS ©-Wireless ©-AAA Enable Uplink Fast Enable Backbone Fast 0 VLAN Members O Spanning Tree O VLAN Setup O VLAN	VLANS		2 Voice 2		$ \in [L] \setminus [L]$		5 P 06			
Qo5 Properties Delete Setup Image: Constraint of the set of	ACLs								Create VLAN	
B - Wireless B - AAA Enable Uplink Fast Enable Backbone Fast Canable Backbone Fast Canable Canable Backbone Fast C	QoS									
Enable Uplink Fast Kanable Backbone Fast Spanning Tree Spanning Tree Spanning Tree Spanning Tree Restrict L2 Traffic Restrict L3 Traffic 	Wireless		Enapping Tree Brones	tion		Pro	Dele	te	Setup	۲
Enable Backbone Fast Enable Backbone Fast	IT HAA		Spanning free Proper						S VLAN Members	
Chable backbone Past			Enable Oplink Past	-						
Restrict L2 Traffic Restrict L3 Traffic			Enable backbone Fast							
Restrict L3 Traffic										
Restrict L3 Traffic									Restrict L2 Traffic	
									Restrict L3 Traffic	
Config: 0 Errors; 2 Warnings Local Changes: none Network Changes: none Alarms 0 0 0 0 0 🚅				Config: 0	Errors; 2 Warnings	Local Changes: none	Network Changes	none Aları	ns 0 0 0 0	0 🛃

10. In the **VLAN Properties** window, disable IGMP by clearing the **Enabled** check box. Click the **OK** button.

🙋 VLAN Properties	8
IGMP	
VLAN IGMP	
Enabled	
Version 2 💌	
Querier Enabled	
Query Interval [seconds]	
Other Querier Present Interval [seconds]	
Query Response Interval [1/10 seconds]	
Last Member Query Interval [1/10 seconds]	
Robustness Value 2	
Proxy Report 🗹	
Multicast Router Solicitation	
Solicitation Interval [seconds] 30	
Help	OK Cancel

Service Profile / SSID configuration

To create a SSID named **Voice** using **WPA-PSK** or **WPA2-PSK** that will be advertised on 802.11a/b/g radios using WMS:

- **1.** In WMS click **Configuration** on the tool bar.
- 2. In the Organizer panel expand the WSS and select Wireless Services.
- 3. In the Network Plan Tasks panel, create a new wireless service by selecting Voice Service Profile.

WMS 6.0: Plan (Polycom	1)							E	
<u>File S</u> ervices <u>T</u> ools H	lelp								
🗢 🔿	a			3		5	9	و ا	
Back Forward	Policies	RF Planning	Configuration	Verification	Devices	Monitor	Alarms	Reports	
Organizer	4	Polycom					5.5 2 10	Network Plan Tasks	4
Polycom						Save		W552360 Changes	
⊡System		Wireless Service Prof	iles						
⊟-Wireless	.	Name	SSID	SSID Type	Bearon	Padio Profile(s)		Review	
Wireless Services		Thanks	5510	SSID Type	Deaton	Radio Honic(a)		Deploy	
Access Points									1
Radios								Create	
RF Detection								802.1X Service Profile	
1 AAA								Voice Service Profile	1
								Web-Portal Service Profile	
								Open Access Service Profile	
								Custom Service Profile	
									- 1
			Config: 1 Err	or; 2 Warnings Lo	al Changes: 1 device	Network Changes:	none Alarr	ns 0 0 0 0 0	-

- **4.** In the **New Voice Service Profile** introduction screen click the **Next** button.
- 5. Specify a Name and SSID for the Voice Service Profile.
- 6. Set the SSID Type to Encrypted and use the default Vendor type SpectraLink. Click the Next button.



Selecting the vendor **SpectraLink** tells WMS what ACLs to create to prioritize the voice traffic later in the wizard.

🖉 Voice Se	ervice Profile			X
Voice SS	ID			
Enter a unio	que name to identify the Service Profile and specify t	the SSID. Also select the voice vendor	.	
Name	Voice]		
SSID	Voice]		
SSID Type	Encrypted -			
Vendor	SpectraLink 💌			
Updated [SSII	D] Value [Voice]			
				The second second second second second
			< Previous Next >	

7. Select the **Open Access** check box. Click the **Next** button.



MAC authentication may optionally be selected but will require that the MAC addresses for each handset be defined in the local AAA database on the WSS.

🙆 Voice Service Profile
Access Types
Choose the types of access you want to allow for this SSID. Select 802.1X Access to allow clients to connect using the IEEE 802.1X standard for authentication, or Select MAC Access to restrict connectivity to known clients based on the client device MAC address, or Open Access to allow clients to connect without per-device authentication.
802.1X Access MAC Access Open Access
Updated [Open Access] Value [Yes]
< Previous Next > Finish Cancel

- 8. Settings for Wireless Security:
 - **a.** To support handsets using WPA-PSK security, select the **WPA** check box.

🔯 Voice Service Profile
Wireless Security
Select one or more wireless security standards. You can configure an SSID to support any combination of RSN, WPA, and non-WPA clients. RSN (sometimes called WPA2) and WPA provide stronger security than WEP.
RSN (WPA2) D WPA V Static WEP D
Updated [WPA] Value [Yes]
< Previous Next > Finish Cancel

b. To support handsets using WPA2-PSK, select the **RSN (WPA2)** check box.

Voice Service Profile
Wireless Security
Select one or more wireless security standards. You can configure an SSID to support any combination of RSN, WPA, and non-WPA clients. RSN (sometimes called WPA2) and WPA provide stronger security than WEP.
RSN (WPA2)
WPA
Static WEP
Updated [WPA] Value [No]
< Previous Next > Finish Cancel

9. Click the **Next** button.

10. Settings for Wireless Encryption Cipher Suite:

a. To support handsets using WPA-PSK with TKIP, select the **TKIP** check box.

🙋 Voice Ser	vice Profile	
Wireless E	Encryption Cipher Suites	
Select one o	r more cipher suites. WPA and RSN support the following cipher suites for packet encryption, listed from most secure to least secure:	
AES (CCMP)	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)-CCMP provides Advanced Encryption Standard (AES) data encryption. To provide message integrity, CCMP uses the Cipher Block Chaining Message Authentication Code (CBC-MAC).	
ТКІР	Temporal Key Integrity Protocol (TKIP)-TKIP uses the RC4 encryption algorithm, a 128-bit encryption key, a 48-bit initialization vector (IV), and a message integrity code (MIC) called Michael	
WEP-104	Wired Equivalent Privacy (WEP) with 104-bit keys-104-bit WEP uses the RC4 encryption algorithm with a 104-bit key.	
WEP-40	U 1WEP with 40-bit keys-40-bit WEP uses the RC4 encryption algorithm with a 40-bit key	
	< Previous Next > Finish Cancel	

b. To support handsets using WPA2-PSK with AES/CCMP, select the **AES (CCMP)** check box and click the **Next** button.

🙋 Voice Ser	vice Profile	
Wireless E	incryption Cipher Suites	
Select one o	r more cipher suites. WPA and RSN support the following cipher suites for packet encryption, listed from most secure to least secure:	
AES (CCMP)	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)-CCMP provides Advanced Encryption Standard (AES) data encryption. To provide message integrity, CCMP uses the Cipher Block Chaining Message Authentication Code (CBC-MAC).	
ТКІР	Temporal Key Integrity Protocol (TKIP)-TKIP uses the RC4 encryption algorithm, a 128-bit encryption key, a 48-bit initialization vector (IV), and a message integrity code (MIC) called Michael	
WEP-104	Uired Equivalent Privacy (WEP) with 104-bit keys-104-bit WEP uses the RC4 encryption algorithm with a 104-bit key.	
WEP-40	UWEP with 40-bit keys-40-bit WEP uses the RC4 encryption algorithm with a 40-bit key	
Updated [TKIP]	Value [No]	
	< Previous Next > Finish Cancel	

11. Enter a hexadecimal pre-shared key or passphrase.

a. If a passphrase is entered, click the **Generate** button to generate the hexadecimal pre-shared key.



The pre-shared key must match on both the WSS and handsets or the handsets will not be able to associate with the Voice SSID.

🖉 Voice Service Profile
Pre-shared Key
Enter the pre-shared key to use for client authentication. To generate a key, enter a pass-phrase and click on Generate
Pre-shared Key enter-a-passphrase
Generate
Enter the pre-shared key in raw nexadecimal form or enter a passphrase (Max Len: 63) to generate a raw key
< Previous Next > Finish Cancel

- **12.** Click the **Next** button.
- **13.** Specify the VLAN named **Voice**. This determines the VLAN that the WSS will map the handset traffic to.
- **14.** Click the **Next** button.

🙋 Voice Service Profile
VLAN
Select a VLAN for clients that connect using this SSID. It is recommended that a separate VLAN be used for voice clients.
VLAN Name Voicel
Updated [VLAN Name] Value [Voice]
< Previous Next > Finish Cancel

15. A default ACL will be generated which will allow and prioritize IP protocol 119 (**SVP**) traffic with the Class of Service level **7** and pass all other IP traffic on the Voice VLAN.

🖉 Void	ce S	ervi	ce Pr	ofile														
QoS:	QoS: SpectraLink (SVP)																	
An AC	An ACL (SpectraLink-1185471492968) has been generated to classify voice traffic. This ACL contains a rule which places all IP protocol 119 (SVP) traffic on Co5																	
queue	queue 7 and a rule that permits all other data traffic on the mapped VLAN (default).																	
ACL -																		
	So	ource	e IP		D	estinati	ion IP		Protocol		Source Port	-	Destination Port	DSCF	, ,	Action	CoS	
· ·		•		/			•	1	svp		any		any 🛃	any		Permit -	7 -	
· ·		•		1				1	any	-	any	-	any 🛃	any	-	Permit 👻	-1	
															Add C		Delete	
														l	AUU P			
Updated	Indated [Protocol Name] Value [svn]																	
	2.10						_											_
													< Previous	Next >		Finish	Cance	

- **a.** (Optional) Modify the default ACL by removing the last statement, which will allow and prioritize IP protocol 119 (SVP) but deny all other IP traffic on the Voice VLAN.
- **16.** Click the **Next** button.

🖉 Voice Service Profile			X							
QoS: SpectraLink (SVP)										
An ACL (SpectraLink-1185501198812) has been generated to classify voice traffic. This ACL contains a rule which places all IP protocol 119 (SVP) traffic on CoS queue 7 and a rule that permits all other data traffic on the mapped VLAN (Voice).										
ACI										
Fourse TD	Destination ID Protocol	Source Part Destination Part DSCD	Action CoS							
	/ svp	any any any any	Permit V 7							
			Add Rule Delete							
undere d Epsere 1 and 1 and Essen 1										
upuaceu (Protocol Namej Value (SVP)	Jpdated [Protocol Name] Value [svp]									
		< Previous Next >	Finish Cancel							

17. Assign the **Voice Service Profile** to the **default** Radio Profile. This will determine which 802.11a and 802.11g radios will advertise the Voice SSID. For this example the default Radio Profile will be used which is assigned to all 802.11a/g radios. This will provide support for handsets operating in 802.11a, 802.11b and 802.11g modes.



All SpectraLink Wireless Telephones on the WLAN network must be configured for a single radio standard (802.11a, or 802.11b, or 802.11g). Handsets configured for different radio standards will not work together.

18. Click the **Finish** button. A Voice Service Profile to support the handsets has now been added to the WSS configuration in WMS.

C Voice Service Profile	
Radio Profile Selection	
Select an existing Radio Profile or choose to create a new one to associate with this Service Profile. Each radio is associated to a single Radio Profile or associate to multiple Service Profiles. This allows a radio to support multiple wireless services.	which can
Create new Radio Profile	
Radio Profiles	
default P	Properties
< Previous Next > Finish	Cancel

Radio Profile configuration

The default Radio Profile needs to be modified to disable certain features to support the handsets. To modify the default Radio Profile using WMS:

- **1.** In WMS click **Configuration** on the tool bar.
- 2. In the Organizer panel expand the WSS and select Radio Profiles.
- **3.** In the **Radio Profiles** list, highlight the **default** Radio Profile and click the **Properties** button.

🙋 WMS 6.	0: Plan (Polycor	m)								
<u>File S</u> erv	rices <u>T</u> ools H	Help								
4			(effe	- K	3		5	9	5	
Back	Forward	Policies	RF Planning	Configuration	Verification	Devices	Monitor	Alarms	Reports	
Organize	7	4	Polycom					5.7	Network Plan Tasks	40
Polycom	.0						Save		W552360 Changes	۲
ė–Sys	tem		Radio Profiles							
⊡Wir	eless		Name	Turne Turnemik D	Turne Cham	nal Associated Can	Ore Made		Review	
	Wireless Service:	s	1 default		V Tune Chan	Voice	SVP	-	Deploy	
	Access Points									
	Radios								Create	8
	RF Detection								Create Radio Profile	
±AA/	4					Pro	perties Dele			
				Config: 0 Erro	ors; 2 Warnings L	ocal Changes: 1 device	Network Changes	none Alarr	ns 0 0 0 0 0	*

- 4. In the Radio Profile Properties window, click the Radio Profile tab.
- **5.** Clear the **Enable Active Scan** check box. This disables active scanning, which prevents the radios from going off-channel and disrupting voice services.

🖉 Radio Profile	e Properties					X
Radio Profile	802.11 Attributes	Auto Tune	Service Profile Selection	Radio Selection	Voice Configuration	1
Radio Profile						
	Name default					
Countermeasur	res Mode None	-				
Enable Act	tive Scan 📃					
Ena	ble RFID					
Enable	U-APSD					

- 6. Click the Auto Tune tab.
- 7. Clear the **Tune Channel** and **Tune Transmit Power** check boxes. This disables automatic channel assignment for radios assigned to the radio profile. A static channel configuration is recommended to provide a stable and optimum RF environment for the handsets.

Radio Profil	e Properties					
Radio Profile	802.11 Attributes	Auto Tune	Service Profile Selection	Radio Selection	Voice Configuration	
Auto Tune –						
	Tune Channe	H 🔲				
	Tune Transmit Powe	r 🗌				
Channel Tur	ing Interval [seconds	3600 🗘				
x. Power Tun	ing Interval [seconds] 600 🔶				
Power Ra	mp Interval [seconds] <u>60</u>				
Channel Tunin	g Holddown [seconds	300				
Tx. Power Ba	ackoff Timer [seconds	10				

- 8. Click the Voice Configuration tab. Verify that the QoS Mode is set to SVP. WMM support is not currently available on the SpectraLink Wireless Telephones.
- 9. Click the **OK** button.

🖉 Radio Profil	e Properties						
Radio Profile	802.11 Attributes	Auto Tune	Service Profile Selection	Radio Selection	Voice Configuration		
Voice Config	wation						
Voice coning							
QoS Mode SV	P 👻						
Help						OK	Cancel

Deploying changes

Deploying the changes in WMS will upload and save the configuration to the WSS. To deploy the changes in WMS:

- 1. In WMS click **Devices** on the tool bar.
- 2. In the Local Changes Task List panel, select **Deploy** to upload and save the configuration changes to the WSS.



You may also $\ensuremath{\textit{Review}}, \ensuremath{\textit{Schedule}}$ and $\ensuremath{\textit{Undo}}$ changes in the Local Changes Task List panel.

🙆 WMS 6.	0: Plan (Poly	ycom)							
<u>File S</u> erv	rices <u>T</u> ools	s Help							
4	-	(<u>_</u>	\mathbb{Z}	3			9	
Back	Forward	Policies	RF Planning	Configuration	Verification	Devices	Monitor	Alarms	Reports
0 2	2								
WSS		IP Address	Managem 🔻 Model	Version	Local St	Network Statu	s	Deploy St	Lund Channel
🛞 Mana	ged Devices	(1)							Local Lhanges 🛞
🖳 WSS23	60 1	.92.168.2.100:8889	Managed 2360	5.0.11.4.0	Changes av C	hecking WSS: Retrying (connection	Completed (T	Review
									🕤 Deploy
									Schedule Deploy
									😌 Undo
									Network Changes 🛞
									Review
									Accept
									🍘 Undo
									Other 🛞
									Refresh
									Upload WSS
									View Operations Log
									Cancel Scheduled Operation
									E Change Management
									Device Operations
				Config: 0 Err	ors; 3 Warnings	.ocal Changes: 1 device	Network Cha	anges: none 🛛 Alarn	ns 2 0 0 0 2 🛃



Deploy configurations				<u> </u>
Mobility Domain 🛆	WSS (Version)		Status	
	WSS2360 (5.0.x)		Deploy completed.	
History WSS/2360: Deploy started. WSS/2360: Sending configuration ch WSS/2360: Applied configuration cha WSS/2360: Saving WSS configuration WSS/2360: Deploy completed.	anges nges 1	Selec	ted Errors	
Deploy completed - 0 failed; 1 succeeded				
Help				⊆lose

3. When the **Deploy** option is selected, WMS will send, apply and save the configuration changes to the WSS.

Example Configuration Files (For Reference Only)

The following configuration file provides an example configuration to support SpectraLink Wireless Telephones using WPA-PSK:

Configuration nvgen'd at 2007-7-26 22:51:55 # Image 5.0.11.4.0 # Model 2360 # Last change occurred at 2007-7-26 22:36:12 set ip route default 192.168.1.1 1 set system name WSS2360 set system ip-address 192.168.1.50 set system countrycode US set timezone EST -5 0 set service-profile Voice ssid-name Voice set service-profile Voice auth-fallthru last-resort set service-profile Voice wpa-ie enable set service-profile Voice psk-phrase enter-a-passphrase set service-profile Voice auth-psk enable set service-profile Voice auth-dot1x disable set service-profile Voice attr vlan-name Voice set enablepass password enable-password set user admin password admin-password set radio-profile default service-profile Voice set radio-profile default dtim-interval 3 set radio-profile default auto-tune channel-config disable set radio-profile default active-scan disable set radio-profile default gos-mode svp set dap 1 serial-id stpw20kc3 model 2330 set dap 1 name WAP-2330-2 set dap 1 radio 1 channel 11 tx-power 10 mode enable set dap 1 radio 2 channel 40 tx-power 10 mode enable set port type ap 1 model 2330 poe enable set ap 1 name WAP-2330-1 set ap 1 radio 1 tx-power 10 mode enable set ap 1 radio 2 channel 44 tx-power 10 mode enable set ip https server enable set port poe 1 enable set vlan 1 name Data set vlan 1 port 8 tag 1

```
set vlan 2 name Voice
set vlan 2 port 8 tag 2
set igmp disable vlan Voice
set interface 1 ip 192.168.1.50 255.255.255.0
set security acl ip SpectraLink permit cos 7 119 0.0.0.0
255.255.255.255 0.0.0.0 255.255.255.255
set security acl ip SpectraLink permit 0.0.0.0
255.255.255.255
commit security acl SpectraLink
set security acl map SpectraLink vlan Voice in
set security acl map SpectraLink vlan Voice out
The following configuration file provides an example configuration to
support SpectraLink Wireless Telephones using WPA2-PSK:
# Configuration nvgen'd at 2007-7-26 22:53:41
# Image 5.0.11.4.0
# Model 2360
# Last change occurred at 2007-7-26 22:53:34
set ip route default 192.168.1.1 1
set system name WSS2360
set system ip-address 192.168.1.50
set system countrycode US
set timezone EST -5 0
set service-profile Voice ssid-name Voice
set service-profile Voice auth-fallthru last-resort
set service-profile Voice rsn-ie enable
set service-profile Voice cipher-tkip disable
set service-profile Voice cipher-ccmp enable
set service-profile Voice psk-phrase enter-a-passphrase
set service-profile Voice auth-psk enable
set service-profile Voice auth-dot1x disable
set service-profile Voice attr vlan-name Voice
set enablepass password enable-password
set user admin password admin-password
set radio-profile default service-profile Voice
set radio-profile default dtim-interval 3
set radio-profile default auto-tune channel-config
disable
set radio-profile default active-scan disable
set radio-profile default gos-mode svp
set dap 1 serial-id stpw20kc3 model 2330
set dap 1 name WAP-2330-2
set dap 1 radio 1 channel 11 tx-power 10 mode enable
```

set dap 1 radio 2 channel 40 tx-power 10 mode enable set port type ap 1 model 2330 poe enable set ap 1 name WAP-2330-1 set ap 1 radio 1 tx-power 10 mode enable set ap 1 radio 2 channel 44 tx-power 10 mode enable set ip https server enable set port poe 1 enable set vlan 1 name Data set vlan 1 port 8 tag 1 set vlan 2 name Voice set vlan 2 port 8 tag 2 set igmp disable vlan Voice set interface 1 ip 192.168.1.50 255.255.255.0 set security acl ip SpectraLink permit cos 7 119 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 set security acl ip SpectraLink permit 0.0.0.0 255.255.255.255 commit security acl SpectraLink set security acl map SpectraLink vlan Voice in set security acl map SpectraLink vlan Voice out